DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Name of MACOM/DA Staff Proponent (APMS Sub Organization Name)

Assistant Chief of Staff for Installation Management (ACSIM), Family & Morale, Welfare and Recreation Command

2. Name of Information Technology (IT) System (APMS System Name)

RecTrac

3. Budget System Identification Number (SNAP-IT Initiative Number)

9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR))

3815

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable)

N/A

6. Privacy Act System of Records Notice Identifier (if applicable)

Pending

7. OMB Information Collection Requirement Number (if applicable) and expiration date

N/A

8. Type of authority to collect information (statutory or otherwise)

10 U.S.C. 3013, Secretary of the Army;
26 U.S.C. 6041, Information at Source;
Army Regulation 215-1, Morale, Welfare and Recreations Activities and Non-appropriated Fund Instrumentalities;
DoD Directive 1015.2, Military Morale, Welfare and Recreation (MWR);
DoD Instruction 1015.10, Program for Military Morale, Welfare and Recreation (MWR);
E.O. 9397 (SSN)
Army Regulation 215-3, Nonappropriated Fund Personnel Policy;
Army Regulation 215-4, Nonappropriated Fund Contracting;
Army Regulation, 608-10 Child Development Services;

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries, and interconnections, location of system and components, and system backup)

RecTrac is the automated customer usage system for MWR. This integrated software system tracks the use of recreational facilities in an effort to provide accurate reporting data. The Army MWR Board of Directors has mandated use of this management information system to provide better recreation service to our customers by monitoring facility and program usage. RecTrac data eventually will be used to determine future funding to support the programs tracked. This system tracks participation in, and use of, sports and fitness centers, swimming pools, craft shops, automotive shops, recreation centers, community activity centers, and live theatre. Individuals complete a one-time registration process. Once registered in RecTrac, customers scan (swipe) their ID cards each time they visit a MWR facility. The RecTrac scanners read the bar codes located on the back of eligible patrons cards.

The purpose of the RecTrac application is to register family members for child development services, track usage, process payments, process annual management reporting and process program registration. RecTrac consists of several modules including, GolfTrac, Child and Youth Management System (CYMS), TeleTrac, WebTrac, e-Rectrac, and MainTrac. It consists of a combination of security, print, file, directory services, application servers, management workstations and the data collection terminals that are used at the various MWR support facilities on the installation.

RecTrac is currently in the sustainment phase of the life cycle process. The system owner is the US Army FMWRC.

RecTrac is a component of the U.S. Army MWR Management Information Systems (MIS), Automated Information Systems (AIS) and MWR Application Service Provider (ASP). The MWR MIS AIS forms a central point of ingress to the base network for MWR activities on that installation. Additionally, the configuration of the MWR MIS AIS is flexible and deployed to meet individual installations program needs using a standard communication methods and a mix of standard MWR software applications.

Backup of system and data files are accomplished weekly, and incremental backups of data files are done daily. These backups are conducted according to instructions provided in the NetWare product documentation.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

The information collected on individuals consists of sponsor name rank and social security number, dependent name, address, date of birth, gender, marital status, household income, housing information, credit card and payment information, userid, passwords, class rosters, pass management files, facility usage data, instructor

information, training and qualifications, activity schedules, resale good inventory, product pricing, menus, rental equipment records, hold harmless agreements for rental contracts, reservation information, account balance information, and revenue from sales data.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.)

Information is collected from Common Access Card (CAC) data sources, face-to-face client interview, supporting documentation supplied by client, product UPC code, keyboard entry by the facility or program manager and keyboard entry by instructors and coaches.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)

The purpose of collecting the data is to properly manage and account for use of facilities and programs and to properly identify authorized users, establish eligibility for services, track usage, process payments, process annual management reporting and process program registration in support of DA Programs and regulatory requirements.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

To register family members for child development services, track usage, process payments, process annual management reporting and to process program registration.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not create new data about individuals through aggregation

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Data collected by this system is shared only with authorized users with a need to know in order to perform official government duties. Routine access to the data in the database is based on the role of the authorized user, *e.g.*, the activity clerks, managers, and MWR system administrators. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

During the initial data collection interview the individual is provided with the Privacy Act Statement and informed that providing the information is optional, and that failure to provide the information may result in slow or denied services. The purpose of collecting data and its uses are described and the individual has the right to refuse to provide the information.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form. See the answer to 16 above.

A Privacy Act Statement is provided at the time the data is collected.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on secure military installations within secured facilities.

The security configuration of the system with the use of access controls, transaction logging, data encryption in transit and at rest and Operating System security enables risk mitigation to an acceptable level and ensures that positive, pro-active preventive measures are in place, as well as suitable forensic measures in the event of a security breach. Access to data is restricted based on need to know. Data access is determined by rights granted and restricted according to user type; both full and incremental backup media are stored securely off-site in fireproof containers. Copies of backup data may be held locally, provided they are similarly secured and protected. Copies of all applications and current patches are kept updated and stored offsite in fireproof containers.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A systems notice currently exists. Either the current notice will be amended to be more descriptive of this business practice, or an entirely new system notice will be developed.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing individual the opportunity to object or consent. The data is encrypted, access to information is controlled by userid and password, user transactions logs maintained and Novell security system is in place. The security measures in place within the security configuration of the system and on the NIPRNET, are in accordance with best practices and due diligence.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.